COMPUTER SCIENCE & TECHNOLOGY:

VALIDATING THE CORRECTNESS OF HARDWARE IMPLEMENTATIONS OF THE NBS DATA ENCRYPTION STANDARD

DEPARTMENT OF COMMERCE ★ NATIONAL BUREAU OF STANDARDS ★

NBS Special Publication 500-20
U.S. DEPARTMENT OF COMMERCE
National Bureau of Standards

NATIONAL BUREAU OF STANDARDS

The National Bureau of Standards[1] was established by an act of Congress March 3, 1901. The Bureau's overall goal is to strengthen and advance the Nation's science and technology and facilitate their effective application for public benefit. To this end, the Bureau conducts research and provides: (1) a basis for the Nation's physical measurement system, (2) scientific and technological services for industry and government, (3) a technical basis for equity in trade, and (4) technical services to promote public safety. The Bureau consists of the Institute for Basic Standards, the Institute for Materials Research, the Institute for Applied Technology, the Institute for Computer Sciences and Technology, the Office for Information Programs, and the Office of Experimental Technology Incentives Program.

THE INSTITUTE FOR BASIC STANDARDS provides the central basis within the United States of a complete and consistent system of physical measurement; coordinates that system with measurement systems of other nations; and furnishes essential services leading to accurate and uniform physical measurements throughout the Nation's scientific community, industry, and commerce. The Institute consists of the Office of Measurement Services, and the following center and divisions:

> Applied Mathematics — Electricity — Mechanics — Heat — Optical Physics — Center for Radiation Research — Laboratory Astrophysics[2] — Cryogenics[2] — Electromagnetics[2] — Time and Frequency[2].

THE INSTITUTE FOR MATERIALS RESEARCH conducts materials research leading to improved methods of measurement, standards, and data on the properties of well-characterized materials needed by industry, commerce, educational institutions, and Government; provides advisory and research services to other Government agencies; and develops, produces, and distributes standard reference materials. The Institute consists of the Office of Standard Reference Materials, the Office of Air and Water Measurement, and the following divisions:

> Analytical Chemistry — Polymers — Metallurgy — Inorganic Materials — Reactor Radiation — Physical Chemistry.

THE INSTITUTE FOR APPLIED TECHNOLOGY provides technical services developing and promoting the use of available technology; cooperates with public and private organizations in developing technological standards, codes, and test methods; and provides technical advice services, and information to Government agencies and the public. The Institute consists of the following divisions and centers:

> Standards Application and Analysis — Electronic Technology — Center for Consumer Product Technology: Product Systems Analysis; Product Engineering — Center for Building Technology: Structures, Materials, and Safety; Building Environment; Technical Evaluation and Application — Center for Fire Research: Fire Science; Fire Safety Engineering.

THE INSTITUTE FOR COMPUTER SCIENCES AND TECHNOLOGY conducts research and provides technical services designed to aid Government agencies in improving cost effectiveness in the conduct of their programs through the selection, acquisition, and effective utilization of automatic data processing equipment; and serves as the principal focus wthin the executive branch for the development of Federal standards for automatic data processing equipment, techniques, and computer languages. The Institute consist of the following divisions:

> Computer Services — Systems and Software — Computer Systems Engineering — Information Technology.

THE OFFICE OF EXPERIMENTAL TECHNOLOGY INCENTIVES PROGRAM seeks to affect public policy and process to facilitate technological change in the private sector by examining and experimenting with Government policies and practices in order to identify and remove Government-related barriers and to correct inherent market imperfections that impede the innovation process.

THE OFFICE FOR INFORMATION PROGRAMS promotes optimum dissemination and accessibility of scientific information generated within NBS; promotes the development of the National Standard Reference Data System and a system of information analysis centers dealing with the broader aspects of the National Measurement System; provides appropriate services to ensure that the NBS staff has optimum accessibility to the scientific information of the world. The Office consists of the following organizational units:

> Office of Standard Reference Data — Office of Information Activities — Office of Technical Publications — Library — Office of International Standards — Office of International Relations.

[1] Headquarters and Laboratories at Gaithersburg, Maryland, unless otherwise noted; mailing address Washington, D.C. 20234.

[2] Located at Boulder, Colorado 80302.

COMPUTER SCIENCE & TECHNOLOGY:

Validating the Correctness of Hardware Implementations of the NBS Data Encryption Standard

Jason Gait

Systems and Software Division
Institute for Computer Sciences and Technology
National Bureau of Standards
Washington, D.C. 20234

U.S. DEPARTMENT OF COMMERCE, Juanita M. Kreps, Secretary

Dr. Sidney Harman, Under Secretary

Jordan J. Baruch, Assistant Secretary for Science and Technology

NATIONAL BUREAU OF STANDARDS, Ernest Ambler, Acting Director

Issued November 1977

Reports on Computer Science and Technology

The National Bureau of Standards has a special responsibility within the Federal Government for computer science and technology activities. The programs of the NBS Institute for Computer Sciences and Technology are designed to provide ADP standards, guidelines, and technical advisory services to improve the effectiveness of computer utilization in the Federal sector, and to perform appropriate research and development efforts as foundation for such activities and programs. This publication series will report these NBS efforts to the Federal computer community as well as to interested specialists in the academic and private sectors. Those wishing to receive notices of publications in this series should complete and return the form at the end of this publication.

National Bureau of Standards Special Publication 500-20
Nat. Bur. Stand. (U.S.), Spec. Publ. 500-20, 46 pages (Nov. 1977)
CODEN: XNBSAV

Library of Congress Catalog Card Number: 77-16067

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON: 1977

For sale by the Superintendent of Documents. U.S. Government Printing Office, Washington, D.C. 20402

Price $1.60 - Stock No. 003-003-01861-9

TABLE OF CONTENTS

LIST OF FIGURES

Validating the Correctness of Hardware Implementations of the NBS Data Encryption Standard

Jason Gait

This publication describes the design and operation of the NBS testbed that is used for the validation of hardware implementations of the Federal Information Processing Data Encryption Standard (DES). A particular implementation is verified if it correctly performs a set of 291 test cases that have been defined to exercise every basic element of the algorithm. As a further check on the correctness of the implementation an extensive Monte-Carlo test is performed. This publication includes the full specification of the DES algorithm, a complete listing of the DES test set and a detailed description of the interface to the testbed.

Key words: Communications security; computer security; cryptography; encryption standard; interface requirements; Monte-Carlo testing; testbed; test cases; validating correctness.

1. INTRODUCTION

The National Bureau of Standards has built a hardware testbed facility to validate manufacturer's implementations of the Federal Information Processing Data Encryption Standard (DES) [3]. The facility includes a hardware implementation of the DES built by NBS in TTL logic and capable of performing an encryption or decryption in 8 micro-seconds. The NBS DES unit is controlled by a microcomputer, which is downstream-loaded with the test program by a time-shared program (currently running on a PDP-11/45 **). When a manufacturer submits a DES device for validation, the device is interfaced to a microcomputer in parallel with the NBS DES unit and its correctness is evaluated by comparison with the NBS DES unit. The device and the NBS DES unit are run

** The designations of computer products contained in this report are included for technical accuracy and completeness. The National Bureau of Standards does not endorse the products of any particular computer manufacturer.

simultaneously and synchronously as the test cases are computed.

Nineteen encryptions and comparisons are required to fully exercise the non-linear substitution tables, or S-boxes. The key schedule is exercised by presenting 56 basis vectors for both encryption and decryption, an additional 112 tests. The initial and final permutations are tested by presenting to each permutation 64 basis vectors, for 128 more tests during which the expansion operator E is automatically verified. The permutation P is verified by performing 32 more encryptions. Thus, a total of 235 encryptions and 56 decryptions are used in the DES test set.

At his option, a manufacturer of a DES implementation may provide an interface to the DES testbed when he submits his device for validation, or NBS will construct the interface from a full specification of device characteristics provided by the manufacturer. If the submitter elects to provide his own interface, he should design it in accordance with the specifications given in this document.

2. DESCRIPTION OF ALGORITHM

The Federal Information Processing Data Encryption Standard published on January 15, 1977 [3] is a complex non-linear ciphering algorithm that was designed with a view to efficient hardware implementation. Although there have been software implementations, they do not comply with the standard and they are generally quite inefficient compared to hardware versions [6]. The DES algorithm operates on 64 bits of plaintext to produce 64 bits of ciphertext under the action of a 56-bit keying parameter. With the exception of initial and final permutations, the algorithm is a series connection of sixteen rounds, one of which is depicted in figure 1. Each round uses 48 bits of the key in a sequence determined by a key schedule. With the exception of this difference in the round keys, the sixteen rounds are identical to one another. Each round receives an input of 64 bits; the 32-bit right half is expanded by the linear operator E to 48 bits and the result is mod two added to the round key; the 48 bit sum is divided into eight 6-bit blocks, each of which determines a 4-bit S-box entry; the resulting 32 bits are added mod two to the left half and the two halves are interchanged, thus producing 64 bits of output for the round. Sixteen rounds connected in series, each using a different round key as determined by the key schedule, together with initial and final permutations make up the DES algorithm. Despite its complexity the DES is capable of operating at high speed when implemented in hardware...for example, an encryption or decryption of one 64-bit block on the NBS DES unit takes 6 micro-seconds. Guidelines on the proper usage of the DES are published in [8].

An example of round-by-round encryption for a given key and plaintext is shown in figure 4. Appendix A contains a complete functional description of the DES algorithm parameters, i. e., permutations, S-boxes and key schedule.

2.1 The Permutations

The role of the permutations is to thoroughly mix the data bits so they cannot be traced back through the S-boxes. Most of the permutations have been designed for efficient hardware realization. In particular, the initial and final permutations are byte oriented, and the controlling microcomputer outputs data to the DES hardware eight bits at a time to take advantage of this feature. In addition to performing a permutation, the operator E expands its 32 bit input to a 48 bit output that is added mod 2 to the round key. The permutation P intermixes the bits that result from the S-box substitution in a complex way to prevent bit tracing. The permutations in the key-schedule intermix the key bits among the round keys in such a way as to equalize key-bit utilization...no key bit is used more than 15 times nor less than 12 times.

Each permutation is a linear operator, and so can be thought of as an n x m matrix and can be completely validated if it operates correctly on an appropriate set of basis vectors. The set of tests for the permutation operators is founded on this principle, and the test cases have been constructed to present a complete set of basis vectors to each operator.

2.2 The S-boxes

The non-linear substitution tables, or S-boxes, constitute the most important part of the algorithm. The purpose of the S-boxes is to ensure that the algorithm is not linear,and hence too weak to stand up under cryptanalytic attack [1,2]. Each of the eight S-boxes, such as is shown in figure 2, contains 64 entries, organized as a 4x16 matrix. Each entry is a four bit binary number, represented as 0-15 in figure 2, so the output of the parallel connection of eight S-boxes is 32 bits. A particular entry in a single S-box is selected by six bits, two of which select a row and four select a column. The entry in the corresponding row and column is the output for that input. Each row in each S-box is a permutation of the numbers 0-15, so no entry is repeated in any one row.

There is no obvious small set of inputs that could be used to verify the S-boxes, so an extensive series of Monte-Carlo experiments was performed to discover a relatively small set of inputs that would exercise every S-box entry at least once. Nearly 200 separate trials were made, and among these were several test sets of 19 inputs which exercised every S-box entry. One of these sets is used as the DES test set for the S-boxes.

2.3 The Key Schedule

The purpose of the key schedule is to provide a thorough intermixing of the key bits for each round. Figure 3 shows how the key schedule determines the sixteen 48-bit round keys from the 56-bit encryption key. The key schedule is linear, so its implementation can be verified by presenting 56 basis vectors as keys, encrypting known input and comparing with known output. The encryption process depends on left shifts in the key schedule, but decryption depends on right shifts, so an additional 56 decryptions are required to test this. The key schedule is extremely important to the security of the algorithm: it has been shown [4] that similar algorithms without key schedules are substanstially weaker, even if they have much larger keys.

3. COMPONENTS OF THE TEST BED

The data encryption testbed has been established within the Institute for Computer Sciences and Technology at the National Bureau of Standards. In order to provide a validation service for DES implementations, the testbed was conceived and developed as a joint effort of ICST's Systems and Software Division and the Computer Systems Engineering Division.

The data encryption testbed was developed in three phases. During phase one the DES algorithm was implemented in readily available TTL hardware technology. Two units are presently in operation. Phase two incorporated these units in a communication channel between a high speed computer terminal and the ICST Computer Facility. A microcomputer is used to interface the NBS DES unit to the data communications channel, as in figure 5. Phase three provided a method of validating commercial data encryption devices implementing the DES.

The most important component of the testbed is the DES algorithm implemented in standard TTL logic. This device performs an encryption or decryption in eignt micro-seconds, and takes 26 micro-seconds to load key or plaintext or to unload ciphertext. This is in contrast to execution times on the order of 30-100 milli-seconds for known software implementations. Figure 6 shows the DES testbed set up for the validation of a manufacturer's DES device. The testbed uses a microcomputer, the NBS DES unit, the proprietary DES device and its interface to the microcomputer port, an operator's terminal (CRT) and a connection to the NBS computer (PDP-11/45). The latter operates in time-sharing mode using the UNIX operating system. The microcomputer contains a small monitor program in read-only memory that is used to permit downstream-loading of the validation software and test data from (PDP-11/45) files under control of the operator's terminal. The current version of the validation software was written and compiled on the PDP-11/45 using an in-house cross-assembler

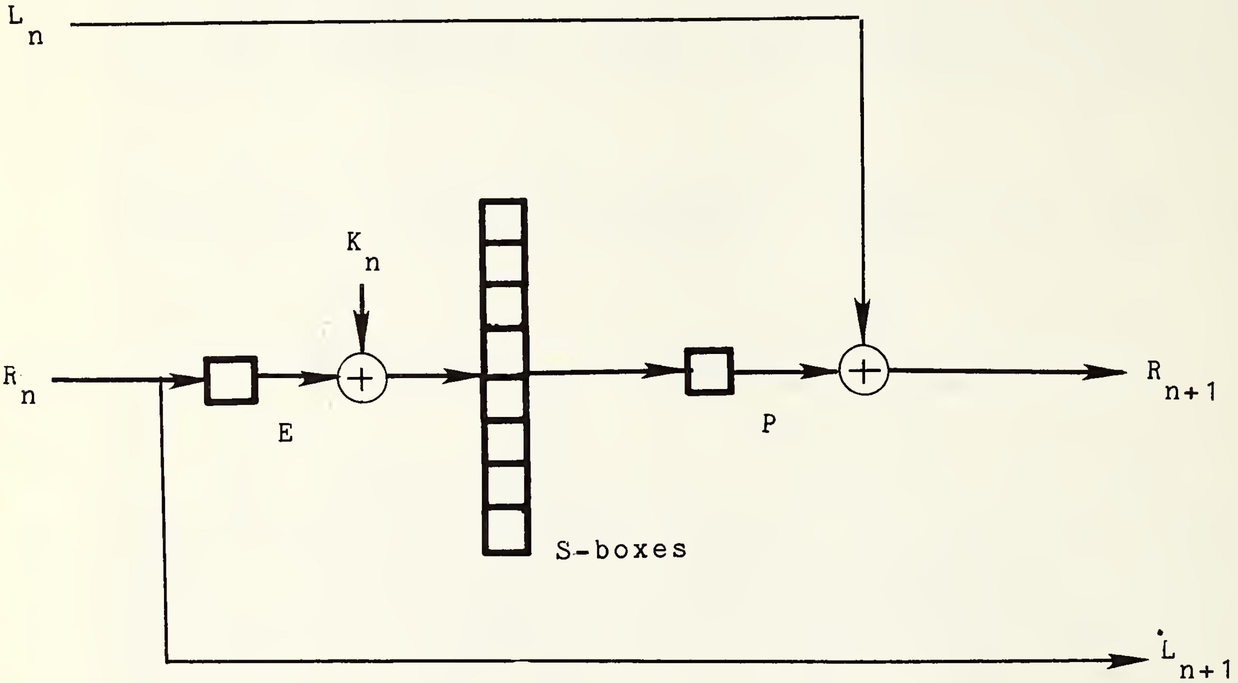


Figure 1 . One of sixteen rounds of the DES. The sixteen rounds are connected in series and have an initial and final permutation.A key schedule determines the round keys.

Figure 2: One of the eight S-boxes in the DES. An S-box entry is determined by a six bit input, four of which determine a column and two determine a row. The output is the four bit S-box entry specified by the row and column. The eight S-boxes are connected in parallel, and are used in each of the sixteen rounds of the DES.

S_1

14	4	13	1	2	15	11	8	3	1Ø	6	12	5	9	Ø	7
Ø	15	7	4	14	2	13	1	1Ø	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	1Ø	5	Ø
15	12	8	2	4	9	1	7	5	11	3	14	1Ø	Ø	6	13

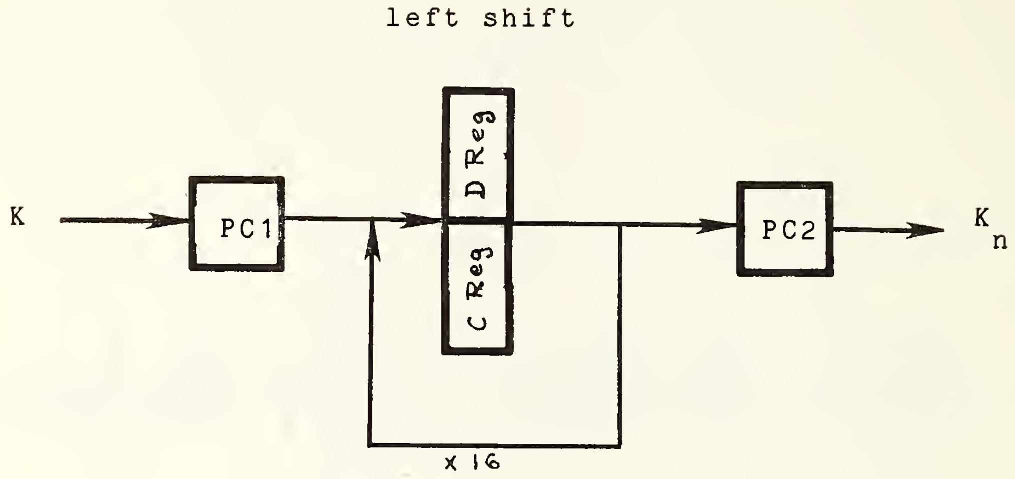


Figure 3 . The key schedule for the DES. The operator PC1 strips away the parity bits from the 64-bit key to produce the 56-bit active key.This is split into two 28 bit registors which are rotated by one or two bits during each round.The operator PC2 produces the 48-bit round key after the bits have been permuted in the registers.

Figure 4: Sample round outputs for the DES. For this example the key is 10316E028C8F3B4A and the plaintext is 0000000000000000.

L	R
00000000	47092B5B
47092B5B	53F372AF
53F372AF	9F1D158B
9F1D158B	8109CBEE
8109CBEE	60448698
60448698	29EBB1A4
29EBB1A4	620CC3A3
620CC3A3	DEEB3D8A
DEEB3D8A	A1A0354D
A1A0354D	9F0303DC
9F0303DC	FD898EE8
FD898EE8	2D1AE1DD
2D1AE1DD	CBC829FA
CBC829FA	B367DEC9
B367DEC9	3F6C3EFD
3F6C3EFD	5A1E5228

OUTPUT

82DCBAFBDEAB6602

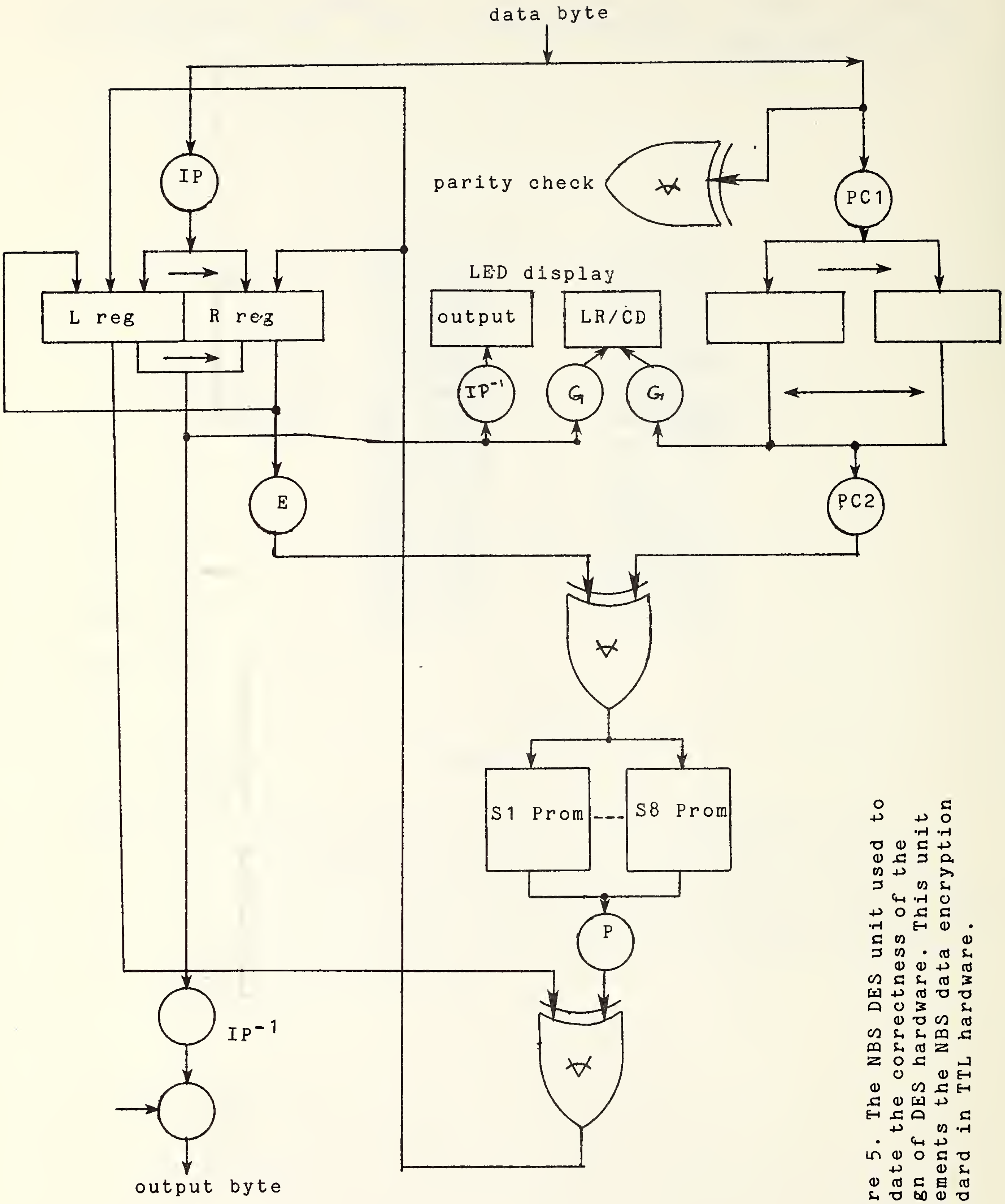


Figure 5. The NBS DES unit used to validate the correctness of the design of DES hardware. This unit implements the NBS data encryption standard in TTL hardware.

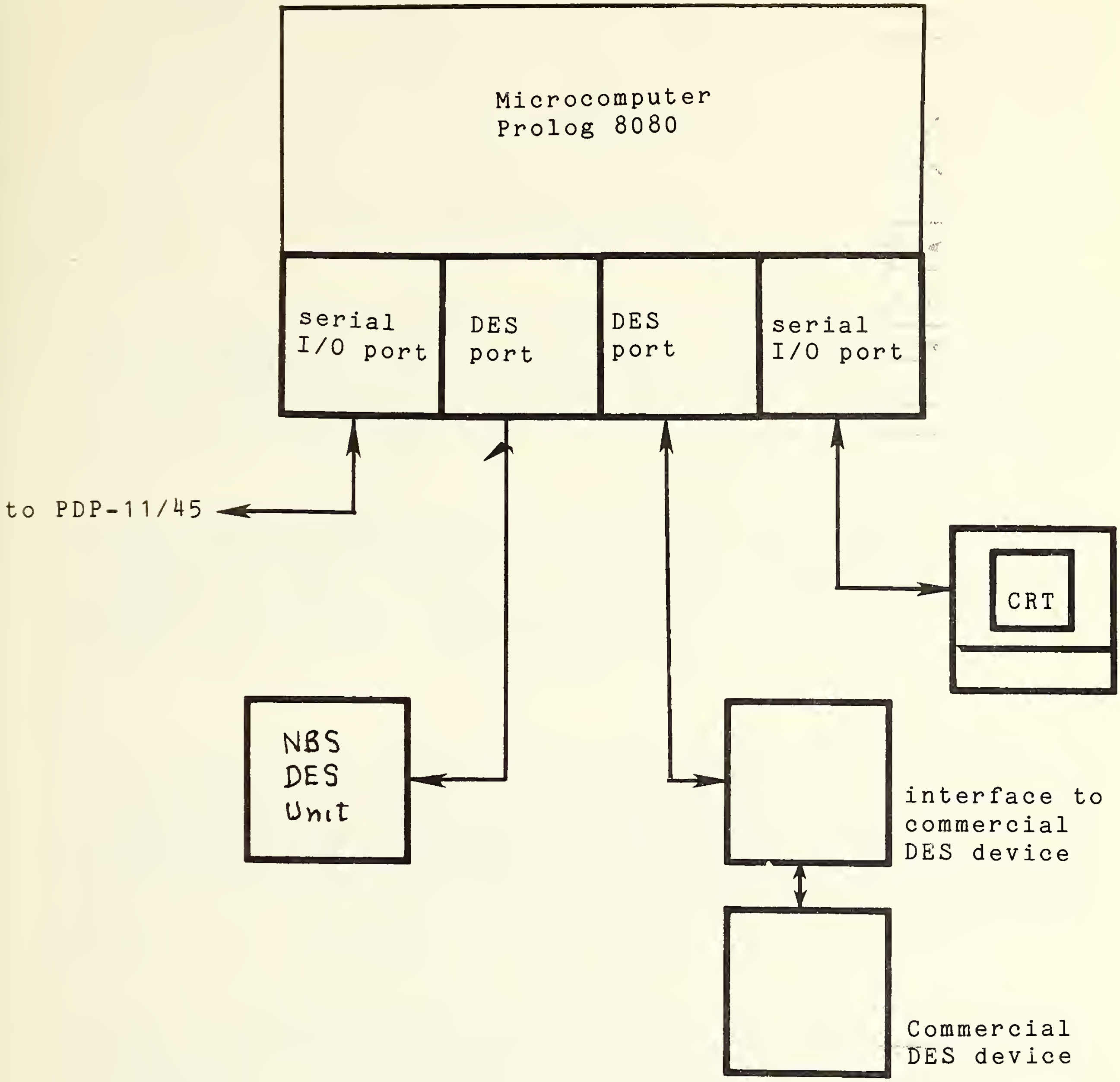


Figure 6 . Current architecture of the validation testbed. The interface can be provided to NBS with the hardware, or it can be built by NBS at cost from specifications of the proprietary hardware.

Figure 7: Sample validation certificate. This certificate is provided by NBS for encryption hardware implementing the DES that has been tested successfully. A prospective vendor of DES encryption equipment to Federal agencies must obtain a certificate of validation.

VALIDATION CERTIFICATE

The National Bureau of Standards has tested an encryption device, identified as............. manufactured by................ in accordance with the specifications of the Data Encryption Standard (FIPS Pub 46) and in accordance with the procedures specified in NBS Special Publication 500-20.

The device has passed the DES test set, and in addition has passed a Monte Carlo test that lasted four million iterations. For the Monte Carlo test the initial value of the key was................. and the initial value of the input was.................... The final value of the key was .... and the final value of the output was ....

Devices bearing the same identification and manufactured to the same design specifications may be labeled as complying with the standard. No reliability test has been performed and no warranty of the devices by the National Bureau of Standards is either expressed or implied.

Dated...................

Signed..................

(Chief, Systems and Software
Division
Institute for Computer Sciences and
Technology, National Bureau of
Standards)

4. THE DEVICE VALIDATION PROCEDURE

The device validation procedure verifies that the manufacturer's hardware design of the DES correctly performs the algorithm. To do this a manufacturer submits a single device from his production line for testing. The validation procedure confirms that the device submitted correctly performs the DES algorithm. Quality control of devices from the production line is the responsibility of the manufacturer. NBS does not certify the reliability of DES devices, only the correctness of the way they implement the DES.

An interface can be provided by NBS for the device submitted or the manufacturer can provide his own interface. The device runs under microcomputer control while performing the encryptions and decryptions of the DES test set, the results being compared to known results in the microcomputer. This test takes less than five minutes. The Monte Carlo test is performed by the commercial device and the NBS device in parallel. This test may run as long as eight hours. The successful completion of the tests will result in the issuance of a validation certificate for the manufacturer's implementation of the DES, and Federal agencies may then purchase identical devices from the manufacturer which are in conformity with the standard.

4.1 The Device/Test-bed Interface

An interface must be designed specifically for each proprietary implementation submitted for validation. This is the most time consuming aspect of the testbed procedure and the manufacturer is required to submit detailed characteristics of his device with regard to voltage levels and operating requirements to facilitate this phase.

The NBS microcomputer interface is designed for use with the NBS DES unit, which uses TTL MSI logic. Firms with commercial implementations of the algorithm that are to be validated by NBS may, at their option, have NBS design and build the necessary interface logic and make necessary software changes to the microcomputer program or they may design their own interface logic that will make their device appear to be identical to the NBS device.

In the former case, it will be necessary to supply adequate documentation to NBS on the operation of the commercial device so that NBS can design the necessary interface logic and software modifications. This documentation should include a definition of all I/O leads, their pin numbers and a narrative description of the operation of the device and of the particular signals needed to operate it. Signal specifications should include the technology to be used by the external circuits (TTL, CMOS, etc.), any external pull-up resistors required, fan out limitations and any unique voltage levels. All power supply voltages needed should be specified. If any of this information is proprietary , this should be so noted.

Full details of the interfacing requirements are included as Appendix C.

4.2 Validating the Implementation

The testbed verifies the correctness of an implementation by performing a series of tests on the device submitted. The tests are chosen to present basis vectors to each of the matrix operators in the algorithm and to exercise every element in each S-box.

4.2.1 Test Procedure. The NBS standard test consists of 291 individual sets of key, plaintext, and ciphertext. The data are stored in a (PDP-11/45) file with each line in the file containing one individual test, e. g.,

```
K0101010101010101   P13213AB764588787   S8000000000000000.
```

The source text of the test program currently resides on a PDP-11/45, and must first be cross-assembled for the PROLOG microcomputer.The resulting object module is downstream loaded into the PROLOG microcomputer via an RS-232 interface. The down- stream loading occurs using a special, almost transparent IO handler on the PROLOG which reads a character from one port (the terminal) and passes it through to the other port (PDP-11/45) and vice versa.

Currently, a program on the PDP-11/45 is executed which starts a process on the PROLOG by sending a special character that starts execution of the test program. The (PDP-11/45) process sends the PROLOG the test data one line at a time. The data is sent in hexadecimal ASCII format . Each line is separated into three sections by tabs and special control characters appear at the beginning of each of these sections. A 'K' at the beginning of the first column indicates that the following 16 characters represent the key. The control character in the second column indicates which operation is to be performed, a 'P' for encryption and a 'S' for decryption. The control character in the third column is the complement of that in the second, indicating that the data following is plaintext or ciphertext.

Once the data has been received, the microcomputer program then loads the test device with the key, followed by the data, and initiates the test. It receives the encrypted or decrypted data back from the test device, and compares it with the expected result. Any deviation in the comparison results in an error message being printed at the console, indicating which individual test failed. The rest of the test is continued. The normal execution time of this test is 3-5 minutes, but it is mainly dependent on the transfer time of the test data, which is transmitted to the PROLOG microcomputer at 240Ø bits per second.

4.2.2 DES Test Set. The tests have been constructed to validate each of the following components of the algorithm:

1. Initial permutation, IP
2. Inverse permutation, IP^{-1}
3. Expansion matrix, E
4. Data Permutation, P
5. Key Permutation, PC1
6. Key Permutation, PC2
7. Substitution tables: $S_1, S_2, \ldots, S_8$

TEST 1: Set Key=Ø and encrypt the 64-bit data vectors

e^i: i=1,...,64; a set of basis vectors.

Basis vectors have all zeros except for a single 1 in the ith position. Compare the resulting cipher c^i with the known results.

CONCLUSIONS: Correct operation verifies the initial permutation, IP. As a full set of basis vectors is also presented to the expansion matrix, E, this operation is also verified.

TEST 2: Set Key=Ø and encrypt the results c^i obtained in TEST 1.

CONCLUSIONS: As the set of basis vectors are recovered, each e^i is presented to the inverse permutation, IP^{-1}, thus verifying it.

TEST 3: To test the permutation operator P, set the plaintext to zero and process the 32 keys in PTEST. This presents a complete set of basis vectors to P.

TEST 4: part 1: Set Data=Ø and use the keys e^i: i=1,...,64 ignoring i=8,16,...,64.

Since the 56 possible basis vectors which yield unique keys are used, this is a complete set of basis vectors for PC1. Compare the results to the known values.

CONCLUSIONS: The key permutation, PC1, is verified. Since the key schedule consists of left shifts, as i ranges over the index set, a complete set of basis vectors is also presented to PC2, so this is verified.

Part 2: set data=c^i from part 1 and use the keys e^i: i=1,...,64 ignoring i=8,16,...64. Then decipher. This tests the right shifts in the key schedule during deciphering.

TEST 5: Set Data and Key equal to the inputs defined in the Substitution Table test. These are a set of 19 key-data pairs that result in every entry of all eight substitution tables being used at least once. Compare the results to the known values.

CONCLUSIONS: The eight substitution tables of 64 entries each are verified.

Appendix B contains a listing of the complete set of standard tests described above.

4.3 Monte-Carlo Testing

Since the test set is known to all, an additional series of tests is performed using pseudo-random data to verify that the device has not been designed just to pass the test set. In addition a successful series of Monte Carlo tests give some assurance that an anomalous combination of inputs does not exist that would cause the device to hang or otherwise malfunction for reasons not directly due to the implementation of the algorithm. While the purpose of the DES test set is to insure that the commercial device performs the DES algorithm accurately, the Monte Carlo test is needed to provide assurance that the commercial device was not built expressly to satisfy the announced tests.

Each device that is submitted for testing is subjected to a Monte-Carlo test on pseudo-random data that will run for a fixed number of iterations for all proprietary devices submitted. An additional purpose of this test is to verify that no undesirable condition within the device will cause the key or plaintext to be exposed in place of ciphertext due to a design error. The Monte-Carlo test is not a reliability test but merely checks for the presence of an apparent operational error. The pseudo-random data is initialized by the test operator at the console, and the test is terminated after a predetermined number of iterations unless there is a failure, in which case the data causing the failure is displayed at the console. The pseudo-random inputs required for the test are produced by the DES itself, used as a pseudo-random number generator. It was shown in [5] that the DES is a statistically good pseudo-random number generator, and the likelihood of cycling is very low during observable time periods.

The Monte-Carlo test, unlike the DES test , runs only on the PROLOG microcomputer. However, the source program is currently kept on a PDP-11/45 and must be cross-assembled and downstream loaded to the PROLOG. Once the program has been loaded, its execution begins immediately. Dialogue consists of prompting the operator for the initial key and seed (plaintext). These are entered as 16 hexadecimal characters. Once this initialization is complete the test begins.

The Monte-Carlo test consists of eight million encryptions and four million decryptions, with one decryption and two encryptions making up a single test. Each of the four million tests is run on both the test device and the NBS DES unit, with comparisons being made after each operation. Each individual test consists of enciphering the plaintext on both the NBS and test devices, comparing the results, enciphering the ciphertext on both the NBS and test device, comparing these results, then deciphering the output of the second encryption on the test device, and comparing this with the first ciphertext. The key remains the same, while the output of the second encryption becomes the new plaintext, as this process is repeated 10,000 times. At this time a new key is generated from the output of the first encryption that occurred in the 10,000th iteration of the preceding group of tests. A message is printed out at the console indicating that the nth group of 10,000 iterations has been completed. This series runs until completion, or until an error is detected. If an error is detected, the current key, the plaintext, the result from the NBS device and the result from the test device is printed out at the console. The error message states whether the error was in the first encryption, the second encryption or the decryption.

This test is allowed to run until four million complete tests, comprising 8 million encipherments and 4 million decipherments , have been generated on the test device. Each group of 10,000 iterations takes approximately one minute to complete, but there will be variations from one proprietary device to another.

4.4 Procedure for Requesting Validation Service

The general policy for validation test procedures is specified in Part 200 of title 15, Code of Federal Regulations, and in the publication "Calibration and Test Services of the National Bureau of Standards" (NBS Special Pub. 250 [7]). Procedures for formally requesting validation services, shipping, testing and preparation and use of the validation certificate are included. Specific instructions for a manufacturer desiring a formal DES validation are provided below.

A formal request for a validation should be sent prior to the time a device is shipped to NBS. This should provide clear identification of the device being submitted, identification of the individual acting as technical representative for the test (i. e., name, address and telephone no.) and instructions for the return of the device. The formal request should also contain authorization to operate the device and authorization to charge for the test. The name and address of the individual to whom the bill should be sent should also be included.

The request for validation, complete specifications of the device to be tested (sufficient for interfacing the device to the DES testbed) and the device itself should be sent to:

Chief, Systems and Software Division
Institute for Computer Sciences and Technology
A-247 Technology Building
National Bureau of Standards
Washington, D. C.,20234

The three items should be sent under separate cover. Inquiries regarding the test should be similarly addressed(or tel. 301-921-3531). The request and specifications should be sent first and the device shipped only after NBS has responded with an estimated cost of validation and a tentative testing schedule.

Insofar as possible, NBS personnel will work jointly with the manufacturer's technical representative in performing a timely test. Special provisions for testing devices that have been integrated into larger electronics equipment will be made as appropriate. Validation of DES devices only assures that the devices correctly implement the DES. The validation procedures do not include reliability testing.

Any device shipped to NBS should be sent in a reuseable container packed to minimize the potential for damage in transit. Shipping and insurance costs must be paid by the manufacturer. NBS will assume no responsibility for damage during shipment, handling or in testing.

A validation certificate will be issued to the manufacturer when the tests are successfully completed. Notification will be made to the technical representative if the tests for any reason cannot be carried out. The tests may be terminated at the request of the manufacturer at any time prior to completion and a bill for costs will be issued.

NBS does not approve, recommend or endorse any commercial product. NBS in no way guarantees that devices similar to the device validated can or will pass the validation tests. However, a manufacturer may certify that devices identical to and bearing the same identification as the device validated implement the DES. Such a claim will make the devices eligible for procurement and use by government agencies. However, no expressed or implied agreement for such procurement is made by NBS.

In accordance with Federal law (15 United States Code 275a), fees are charged for all measurement services performed by the National Bureau of Standards. Fees will include the cost of labor and materials used in performing the validation tests and in issuing a validation certificate. Labor costs will include administrative, engineering and programming personnel participating in the test. Labor rates will be determined by the cost of the personnel, including applicable overhead. Materials cost will be actual cost to NBS. Travel costs, when necessary, will be actual costs to NBS. Bills will be issued upon completion or termination of the test. A validation certificate will be issued upon receipt of payment.

5. PREPARATION OF DEVICE VALIDATION REPORT

Each manufaturer who submits an implementation for validation will receive a validation certificate detailing the results of the standard test and of the Monte-Carlo test. The successful performance of the tests and the submission of a properly completed validation certificate on the part of the manufacturer is required by the Federal Government in all cases where procurement is being considered by a Federal agency or department. A typical validation certificate will state that the device submitted by the manufacturer satisfied the DES test set, and will also give the starting parameters and final results for the Monte-Carlo test, so the test can be exactly repeated in the future should any question arise. A sample validation certificate is shown in figure 7.

ACKNOWLEDGEMENTS

Dana Grubb and Lou Palombo, of the Computer Systems Engineering Division, designed and constructed the NBS DES unit. Joe Sokol, of the Systems and Software Division, was responsible for the production of the testbed software. William Truitt, of the Computer Systems Engineering Division , adapted and interfaced the microcomputer for the testbed.

Dennis Branstad, of the Systems and Software Division, was responsible for the conception and overall design of the DES testbed. Seymour Jeffery, Chief of the Systems and Software Division, has provided consistent support for the project since its inception.

Thomas N. Pyke, Jr., Chief of the Computer Systems Engineering Division, provided guidance on the design of the validation certificate. Gordon Fields, Staff Attorney in the NBS Legal Office, provided many suggestions.

APPENDICES

6. Appendix A: The DES Algorithm Specification

For the convenience of the reader, this appendix contains a complete specification of the parameters involved in the definition of the DES algorithm.

The DES acts on a 64 bit block of plaintext, which is first permuted by IP:

IP

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

(e. g., bit one of the output is bit 58 of the input and bit two is bit 50, etc.)

The result is separated into two 32 bit registers, L and R, and then passed through the sixteen rounds as in figure A1. The final 64 bit result is operated on by the inverse of IP, IP^{-1}:

IP^{-1}

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

The round keys K_n are determined by the key schedule that is diagrammed in figure 3. There are three parameters to be specified, PC1, PC2 and the shift schedule:

PC1

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

PC2

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

and the shift schedule is:

Iteration	Number of shifts
1	1
2	1
3	2
4	2

5	2
6	2
7	2
8	2
9	1
10	2
11	2
12	2
13	2
14	2
15	2
16	1

For a single round the expansion operator E and the permutation P need to be specified:

E

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

P

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

There remain only the S-boxes:

(S_1 is figure 2.)

S_2

15	1	8	14	6	11	3	4	9	7	2	13	12	Ø	5	1Ø
3	13	4	7	15	2	8	14	12	Ø	1	1Ø	6	9	11	5
Ø	14	7	11	1Ø	4	13	1	5	8	12	6	9	3	2	15
13	8	1Ø	1	3	15	4	2	11	6	7	12	Ø	5	14	9

S_3

1Ø	Ø	9	14	6	3	15	5	1	13	12	7	11	4	2	8
13	7	Ø	9	3	4	6	1Ø	2	8	5	14	12	11	15	1
13	6	4	9	8	15	3	Ø	11	1	2	12	5	1Ø	14	7
1	1Ø	13	Ø	6	9	8	7	4	15	14	3	11	5	2	12

S_4

7	13	14	3	Ø	6	9	1Ø	1	2	8	5	11	12	4	15
13	8	11	5	6	15	Ø	3	4	7	2	12	1	1Ø	14	9
1Ø	6	9	Ø	12	11	7	13	15	1	3	14	5	2	8	4
3	15	Ø	6	1Ø	1	13	8	9	4	5	11	12	7	2	14

S_5

2	12	4	1	7	1Ø	11	6	8	5	3	15	13	Ø	14	9
14	11	2	12	4	7	13	1	5	Ø	15	1Ø	3	9	8	6
4	2	1	11	1Ø	13	7	8	15	9	12	5	6	3	Ø	14
11	8	12	7	1	14	2	13	6	15	Ø	9	1Ø	4	5	3

S_6

12	1	1Ø	15	9	2	6	8	Ø	13	3	4	14	7	5	11

10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

S_7

4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

S_8

13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

The reader is referred to [3] for the official specification of these parameters.

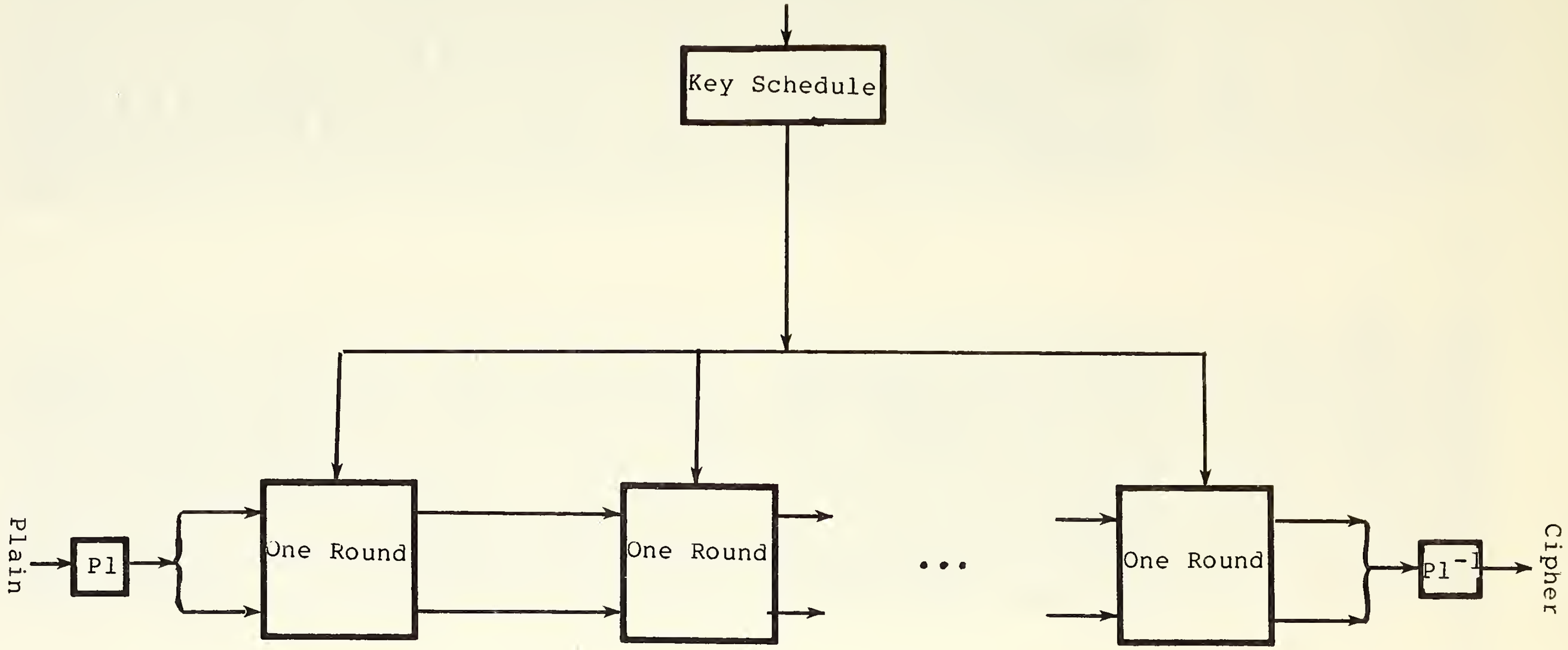


Figure A1 . The sixteen rounds of the DES. The rounds are connected in series with initial and final permutations. The round keys are determined by a key schedule that is described elsewhere.

7. Appendix B: The DES Test Set

IP AND E TEST

KEY	PLAIN	CIPHER
0101010101010101	95F8A5E5DD31D900	8000000000000000
0101010101010101	DD7F121CA5015619	4000000000000000
0101010101010101	2E8653104F3834EA	2000000000000000
0101010101010101	4BD388FF6CD81D4F	1000000000000000
0101010101010101	20B9E767B2FB1456	0800000000000000
0101010101010101	55579380D77138EF	0400000000000000
0101010101010101	6CC5DEFAAF04512F	0200000000000000
0101010101010101	0D9F279BA5D87260	0100000000000000
0101010101010101	D9031B0271BD5A0A	0080000000000000
0101010101010101	424250B37C3DD951	0040000000000000
0101010101010101	B8061B7ECD9A21E5	0020000000000000
0101010101010101	F15D0F286B65BD28	0010000000000000
0101010101010101	ADD0CC8D6E5DEBA1	0008000000000000
0101010101010101	E6D5F82752AD63D1	0004000000000000
0101010101010101	ECBFE3BD3F591A5E	0002000000000000
0101010101010101	F356834379D165CD	0001000000000000
0101010101010101	2B9F982F20037FA9	0000800000000000
0101010101010101	889DE068A16F0BE6	0000400000000000
0101010101010101	E19E275D846A1298	0000200000000000
0101010101010101	329A8ED523D71AEC	0000100000000000
0101010101010101	E7FCE22557D23C97	0000080000000000
0101010101010101	12A9F5817FF2D65D	0000040000000000
0101010101010101	A484C3AD38DC9C19	0000020000000000
0101010101010101	FBE00A8A1EF8AD72	0000010000000000
0101010101010101	750D079407521363	0000008000000000
0101010101010101	64FEED9C724C2FAF	0000004000000000
0101010101010101	F02B263B328E2B60	0000002000000000
0101010101010101	9D64555A9A10B852	0000001000000000
0101010101010101	D106FF0BED5255D7	0000000800000000
0101010101010101	E1652C6B138C64A5	0000000400000000
0101010101010101	E428581186EC8F46	0000000200000000
0101010101010101	AEB5F5EDE22D1A36	0000000100000000
0101010101010101	E943D7568AEC0C5C	0000000080000000
0101010101010101	DF98C8276F54B04B	0000000040000000
0101010101010101	B160E4680F6C696F	0000000020000000
0101010101010101	FA0752B07D9C4AB8	0000000010000000
0101010101010101	CA3A2B036DBC8502	0000000008000000
0101010101010101	5E0905517BB59BCF	0000000004000000
0101010101010101	814EEB3B91D90726	0000000002000000
0101010101010101	4D49DB1532919C9F	0000000001000000

Ø1Ø1Ø1Ø1Ø1Ø1Ø1Ø1	25EB5FC3F8CFØ621	ØØØØØØØØØØ8ØØØØØ
Ø1Ø1Ø1Ø1Ø1Ø1Ø1Ø1	AB6A2ØCØ62ØD1C6F	ØØØØØØØØØØ4ØØØØØ
Ø1Ø1Ø1Ø1Ø1Ø1Ø1Ø1	79E9ØDBC98F92CCA	ØØØØØØØØØØ2ØØØØØ
Ø1Ø1Ø1Ø1Ø1Ø1Ø1Ø1	866ECEDD8Ø72BBØE	ØØØØØØØØØØ1ØØØØØ
Ø1Ø1Ø1Ø1Ø1Ø1Ø1Ø1	8B54536F2F3E64A8	ØØØØØØØØØØØ8ØØØØ
Ø1Ø1Ø1Ø1Ø1Ø1Ø1Ø1	EA51D3975595B86B	ØØØØØØØØØØØ4ØØØØ
Ø1Ø1Ø1Ø1Ø1Ø1Ø1Ø1	CAFFC6AC4542DE31	ØØØØØØØØØØØ2ØØØØ
Ø1Ø1Ø1Ø1Ø1Ø1Ø1Ø1	8DD45A2DDF9Ø796C	ØØØØØØØØØØØ1ØØØØ
Ø1Ø1Ø1Ø1Ø1Ø1Ø1Ø1	1Ø29D55E88ØEC2DØ	ØØØØØØØØØØØØ8ØØØ
Ø1Ø1Ø1Ø1Ø1Ø1Ø1Ø1	5D86CB23639DBEA9	ØØØØØØØØØØØØ4ØØØ
Ø1Ø1Ø1Ø1Ø1Ø1Ø1Ø1	1D1CA853AE7CØC5F	ØØØØØØØØØØØØ2ØØØ
Ø1Ø1Ø1Ø1Ø1Ø1Ø1Ø1	CE332329248F3228	ØØØØØØØØØØØØ1ØØØ
Ø1Ø1Ø1Ø1Ø1Ø1Ø1Ø1	84Ø5D1ABE24FB942	ØØØØØØØØØØØØØ8ØØ
Ø1Ø1Ø1Ø1Ø1Ø1Ø1Ø1	E643D78Ø9ØCA42Ø7	ØØØØØØØØØØØØØ4ØØ
Ø1Ø1Ø1Ø1Ø1Ø1Ø1Ø1	48221B9937748A23	ØØØØØØØØØØØØØ2ØØ
Ø1Ø1Ø1Ø1Ø1Ø1Ø1Ø1	DD7CØBBD61FAFD54	ØØØØØØØØØØØØØ1ØØ
Ø1Ø1Ø1Ø1Ø1Ø1Ø1Ø1	2FBC291A57ØDB5C4	ØØØØØØØØØØØØØØ8Ø
Ø1Ø1Ø1Ø1Ø1Ø1Ø1Ø1	EØ7C3ØD7E4E26E12	ØØØØØØØØØØØØØØ4Ø
Ø1Ø1Ø1Ø1Ø1Ø1Ø1Ø1	Ø953E2258E8E9ØA1	ØØØØØØØØØØØØØØ2Ø
Ø1Ø1Ø1Ø1Ø1Ø1Ø1Ø1	5B711BC4CEEBF2EE	ØØØØØØØØØØØØØØ1Ø
Ø1Ø1Ø1Ø1Ø1Ø1Ø1Ø1	CCØ83F1E6D9E85F6	ØØØØØØØØØØØØØØØ8
Ø1Ø1Ø1Ø1Ø1Ø1Ø1Ø1	D2FD8867D5ØD2DFE	ØØØØØØØØØØØØØØØ4
Ø1Ø1Ø1Ø1Ø1Ø1Ø1Ø1	Ø6E7EA22CE927Ø8F	ØØØØØØØØØØØØØØØ2
Ø1Ø1Ø1Ø1Ø1Ø1Ø1Ø1	166B4ØB44ABA4BD6	ØØØØØØØØØØØØØØØ1

PC1 AND PC2 TEST

KEY	PLAIN	CIPHER
8001010101010101	0000000000000000	95A8D72813DAA94D
4001010101010101	0000000000000000	0EEC1487DD8C26D5
2001010101010101	0000000000000000	7AD16FFB79C45926
1001010101010101	0000000000000000	D3746294CA6A6CF3
0801010101010101	0000000000000000	809F5F873C1FD761
0401010101010101	0000000000000000	C02FAFFEC989D1FC
0201010101010101	0000000000000000	4615AA1D33E72F10
0180010101010101	0000000000000000	2055123350C00858
0140010101010101	0000000000000000	DF3B99D6577397C8
0120010101010101	0000000000000000	31FE17369B5288C9
0110010101010101	0000000000000000	DFDD3CC64DAE1642
0108010101010101	0000000000000000	178C83CE2B399D94
0104010101010101	0000000000000000	50F636324A9B7F80
0102010101010101	0000000000000000	A8468EE3BC18F06D
0101800101010101	0000000000000000	A2DC9E92FD3CDE92
0101400101010101	0000000000000000	CAC09F797D031287
0101200101010101	0000000000000000	90BA680B22AEB525
0101100101010101	0000000000000000	CE7A24F350E280B6
0101080101010101	0000000000000000	882BFF0AA01A0B87
0101040101010101	0000000000000000	25610288924511C2
0101020101010101	0000000000000000	C71516C29C75D170
0101018001010101	0000000000000000	5199C29A52C9F059
0101014001010101	0000000000000000	C22F0A294A71F29F
0101012001010101	0000000000000000	EE371483714C02EA
0101011001010101	0000000000000000	A81FBD448F9E522F
0101010801010101	0000000000000000	4F644C92E192DFED
0101010401010101	0000000000000000	1AFA9A66A6DF92AE
0101010201010101	0000000000000000	B3C1CC715CB879D8
0101010180010101	0000000000000000	19D032E64AB0BD8B
0101010140010101	0000000000000000	3CFAA7A7DC8720DC
0101010120010101	0000000000000000	B7265F7F447AC6F3
0101010110010101	0000000000000000	9DB73B3C0D163F54
0101010108010101	0000000000000000	8181B65BABF4A975
0101010104010101	0000000000000000	93C9B64042EAA240
0101010102010101	0000000000000000	5570530829705592
0101010101800101	0000000000000000	8638809E878787A0
0101010101400101	0000000000000000	41B9A79AF79AC208
0101010101200101	0000000000000000	7A9BE42F2009A892
0101010101100101	0000000000000000	29038D56BA6D2745
0101010101080101	0000000000000000	5495C6ABF1E5DF51
0101010101040101	0000000000000000	AE13DBD561488933
0101010101020101	0000000000000000	024D1FFA8904E389

0101010101018001	0000000000000000	D1399712F99BF02E
0101010101014001	0000000000000000	14C1D7C1CFFEC79E
0101010101012001	0000000000000000	1DE5279DAE3BED6F
0101010101011001	0000000000000000	E941A33F85501303
0101010101010801	0000000000000000	DA99DBBC9A03F379
0101010101010401	0000000000000000	B7FC92F91D8E92E9
0101010101010201	0000000000000000	AE8E5CAA3CA04E85
0101010101010180	0000000000000000	9CC62DF43B6EED74
0101010101010140	0000000000000000	D863DBB5C59A91A0
0101010101010120	0000000000000000	A1AB2190545B91D7
0101010101010110	0000000000000000	0875041E64C570F7
0101010101010108	0000000000000000	5A594528BEBEF1CC
0101010101010104	0000000000000000	FCDB3291DE21F0C0
0101010101010102	0000000000000000	869EFD7F9F265A09

PTEST

KEY	PLAIN	CIPHER
1046913489980131	0000000000000000	88D55E54F54C97B4
1007103489988020	0000000000000000	0C0CC00C83EA48FD
10071034C8980120	0000000000000000	83BC8EF3A6570183
1046103489988020	0000000000000000	DF725DCAD94EA2E9
1086911519190101	0000000000000000	E652B53B550BE8B0
1086911519580101	0000000000000000	AF527120C485CBB0
5107B01519580101	0000000000000000	0F04CE393DB926D5
1007B01519190101	0000000000000000	C9F00FFC74079067
3107915498080101	0000000000000000	7CFD82A593252B4E
3107919498080101	0000000000000000	CB49A2F9E91363E3
10079115B9080140	0000000000000000	00B588BE70D23F56
3107911598080140	0000000000000000	406A9A6AB43399AE
1007D01589980101	0000000000000000	6CB773611DCA9ADA
9107911589980101	0000000000000000	67FD21C17DBB5D70
9107D01589190101	0000000000000000	9592CB4110430787
1007D01598980120	0000000000000000	A6B7FF68A318DDD3
1007940498190101	0000000000000000	4D102196C914CA16
0107910491190401	0000000000000000	2DFA9F4573594965
0107910491190101	0000000000000000	B46604816C0E0774
0107940491190401	0000000000000000	6E7E6221A4F34E87
19079210981A0101	0000000000000000	AA85E74643233199
1007911998190801	0000000000000000	2E5A19DB4D1962D6
10079119981A0801	0000000000000000	23A866A809D30894
1007921098190101	0000000000000000	D812D961F017D320
100791159819010B	0000000000000000	055605816E58608F
1004801598190101	0000000000000000	ABD88E8B1B7716F1
1004801598190102	0000000000000000	537AC95BE69DA1E1
1004801598190108	0000000000000000	AED0F6AE3C25CDD8
1002911598100104	0000000000000000	B3E35A5EE53E7B8D
1002911598190104	0000000000000000	61C79C71921A2EF8
1002911598100201	0000000000000000	E2F5728F0995013C
1002911698100101	0000000000000000	1AEAC39A61F0A464

19 Key data pairs which exercise every S-box entry.

KEY	PLAIN	CIPHER
7CA110454A1A6E57	01A1D6D039776742	690F5B0D9A26939B
0131D9619DC1376E	5CD54CA83DEF57DA	7A389D10354BD271
07A1133E4A0B2686	0248D43806F67172	868EBB51CAB4599A
3849674C2602319E	51454B582DDF440A	7178876E01F19B2A
04B915BA43FEB5B6	42FD443059577FA2	AF37FB421F8C4095
0113B970FD34F2CE	059B5E0851CF143A	86A560F10EC6D85B
0170F175468FB5E6	0756D8E0774761D2	0CD3DA020021DC09
43297FAD38E373FE	762514B829BF486A	EA676B2CB7DB2B7A
07A7137045DA2A16	3BDD119049372802	DFD64A815CAF1A0F
04689104C2FD3B2F	26955F6835AF609A	5C513C9C4886C088
37D06BB516CB7546	164D5E404F275232	0A2AEEAE3FF4AB77
1F08260D1AC2465E	6B056E18759F5CCA	EF1BF03E5DFA575A
584023641ABA6176	004BD6EF09176062	88BF0DB6D70DEE56
025816164629B007	480D39006EE762F2	A1F9915541020B56
49793EBC79B3258F	437540C8698F3CFA	6FBF1CAFCFFD0556
4FB05E1515AB73A7	072D43A077075292	2F22E49BAB7CA1AC
49E95D6D4CA229BF	02FE55778117F12A	5A6B612CC26CCE4A
018310DC409B26D6	1D9D5C5018F728C2	5F4C038ED12B2E41
1C587F1C13924FEF	305532286D6F295A	63FAC0D034D9F793

8. Appendix C: Interface Specifications

A manufacturer providing his own interface logic should use the following description and attached diagrams . In some cases, it will be relatively easy to provide hardwired logic that will make the device appear to be identical to the NBS device. However, there may be cases where it will not be feasible to make the device appear identical without software modifications in the microcomputer. In these cases, NBS personnel will make the necessary changes on a cost reimbursable basis.

Interface Design

The interface uses TTL logic levels (high-level output voltage of at least plus 2.4 volts and low-level of not more than plus Ø.4 volts). The cabling normally provides a twisted pair return on three control lines to minimize the effect of noise. If further noise problems should arise, there are connector pins already allocated for twisted pair returns on the other lines. The connector uses an ELCO plug, part number ØØ-8Ø16-Ø56-ØØØ-819. In most cases it will be easier if NBS provides the connector plug and wires it as per the pin assignments of the proprietary device. If desired, the submitter may use a different connector, provided that he supplies NBS with a mate to the connector for cabling to the ELCO on the NBS microcomputer.

The lines used in the interface are shown in figure Cl and salient interface logic in figure C2. These lines are used for transferring a byte of data or key into the device from the microcomputer, for transferring a byte of data from the device back to the microcomputer and for various other control functions.

The mode of operation is controlled by the two lines: DATA/KEY and ENCIPHER/DECIPHER DATA. These levels will be stationary during a given operation. Thus, the proprietary device may either sample them at the time the first byte is loaded (data or key) or merely use them as levels for control of the process. (NBS uses the first alternative in its implementation to avoid the chance of any noise on the lines causing a malfunction.) The DATA/KEY line is low when a block of data is to be enciphered or deciphered. It is high when the key is entered. The ENCIPHER/DECIPHER DATA line is examined by the device only when data is to be enciphered or deciphered; otherwise it must be ignored. The key is always loaded in the clear in the validation tests, so any proprietary features for enciphering or deciphering of the key should be inactive during the tests. (However, each option of the proprietary device may be tested by making special arrangements with NBS.)

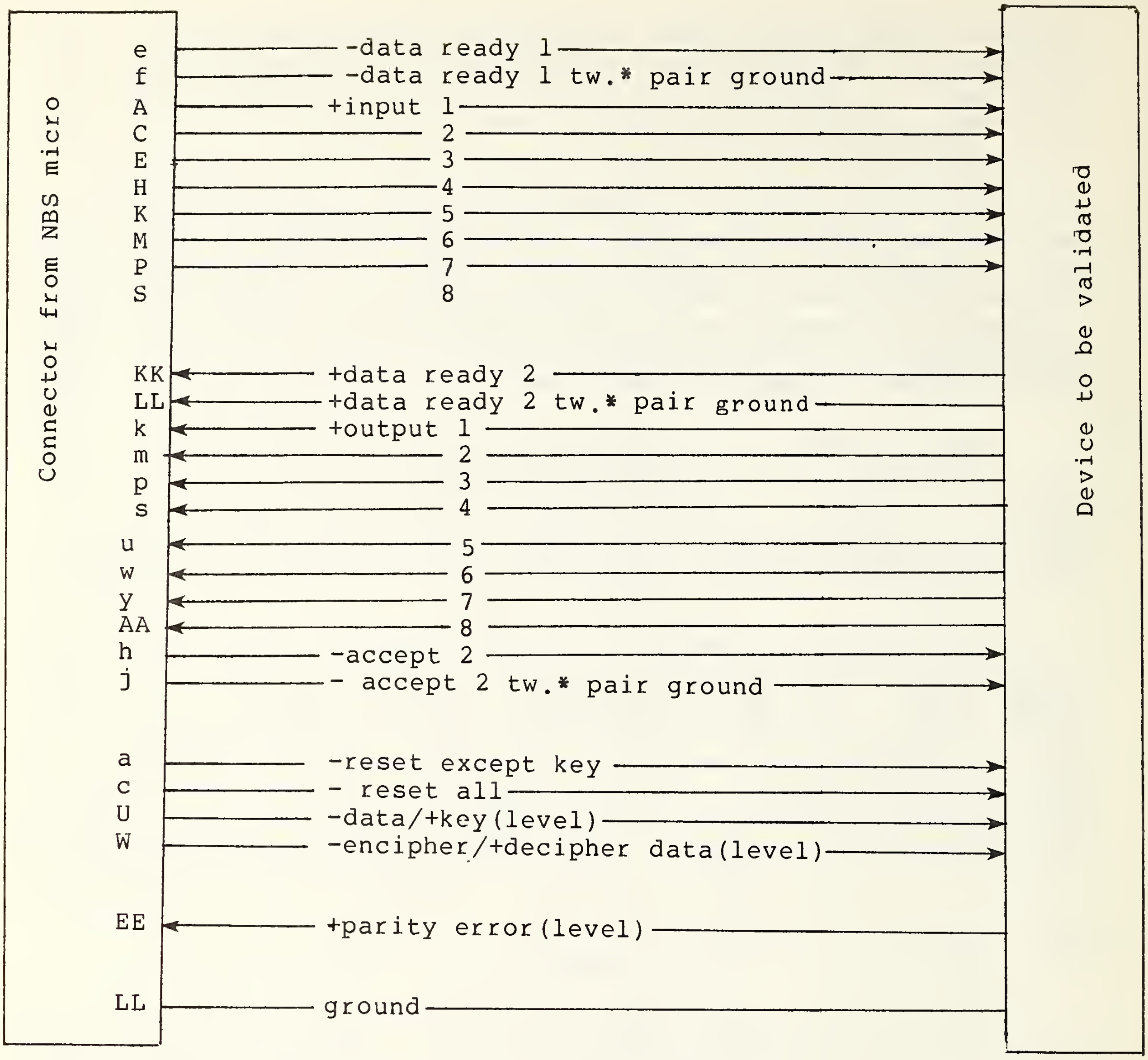
The RESET EXCEPT KEY level is set by the microcomputer program and then reset by a subsequent instruction. It is used to reset the controls in the device. It may, optionally, be used to reset the LR Register, though this is not necessary. The RESET ALL signal (level) was used in the NBS implementation as a convenience for demonstration purposes and need not be implemented.

PARITY ERROR is a level from the proprietary device that indicates that one or more bytes of the key have even parity. However, it does not have to be implemented. Some devices may have available additional status indicators like BUSY and CONTROL ERROR. The tests do not make use of these indicators.

The lines for loading a byte of data or key into the device are DATA READY 1, its twisted pair return and the 8 INPUT lines. The NBS microcomputer sets up the 8 INPUT lines and, in a subsequent instruction, fires a one shot to give an approximate one microsecond pulse for DATA READY 1. The device should use DATA READY 1 to strobe the 8 INPUT lines into the device. No response from the device to the microcomputer is needed. The 8 INPUT lines should be loaded as data or as key depending on the status of the DATA/KEY control line described previously. This process is repeated for each of the 8 bytes required for the 64 bits of data or key to be loaded into the device.

The lines for transferring a byte of data back to the microcomputer are DATA READY 2, ACCEPT 2, their twisted pair returns, and the 8 OUTPUT lines. This transfer is asynchronous due to the much slower speed of the microcomputer. The sequence is: DATA READY 2 goes active (high) from the device after the 8 OUTPUT lines are stabilized; the DATA READY 2 line is polled by the program; a subsequent instruction fires a one shot to give an approximately one microsecond pulse for ACCEPT 2 (active low) to the device; and the device brings DATA READY 2 inactive (low) in response to ACCEPT 2. This process is repeated for each of the 8 bytes required for a 64 bit block transfer.

The input data, input key and output data byte numbering are shown in the figures C3 and C4.



*twisted

Figure C1 . Interface line specifications or the NBS data encryption testbed.

Cable pluy; ELCO 00-8016-056-000-819

Chassis socket: ELCO 00-8016-056-000-707

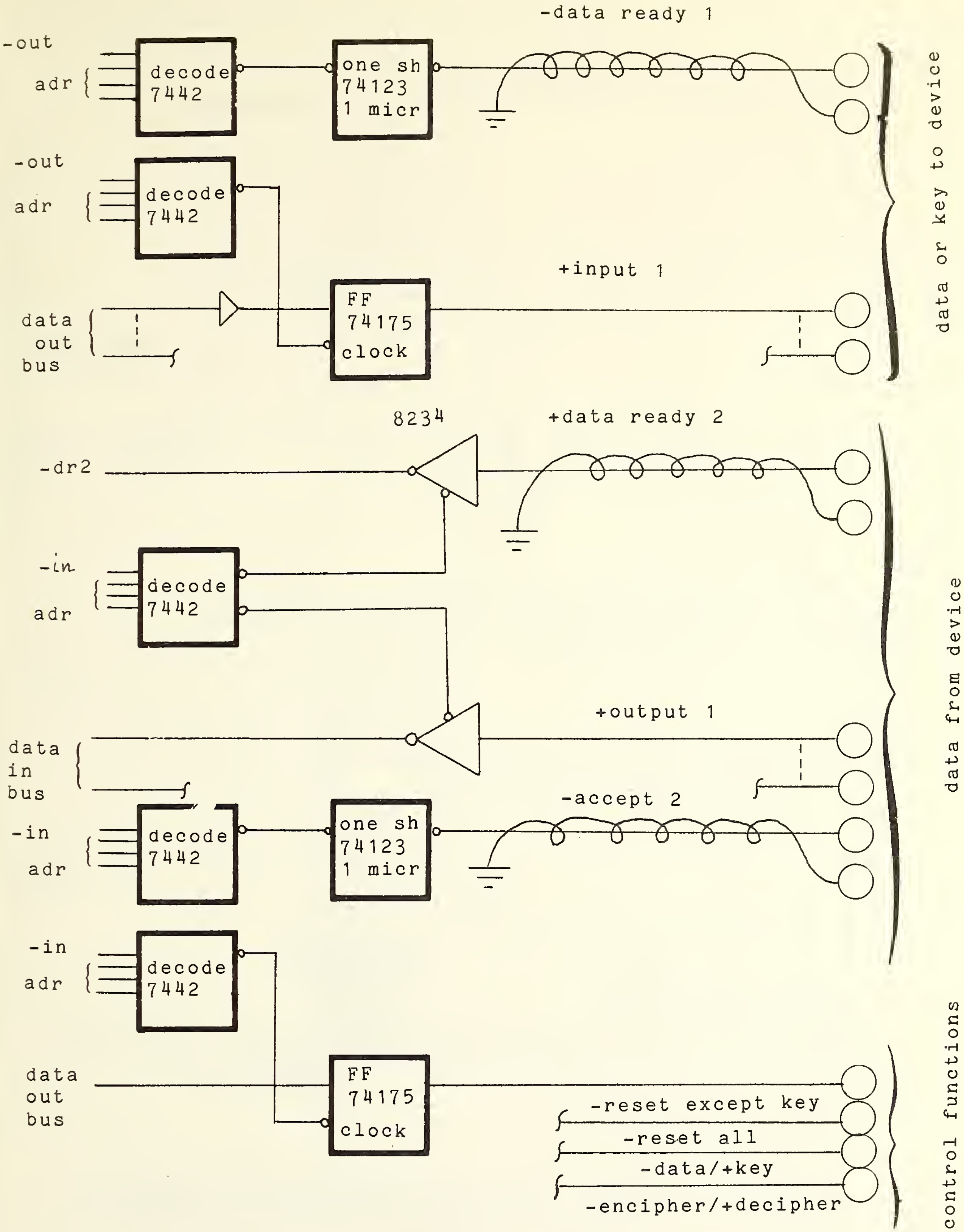
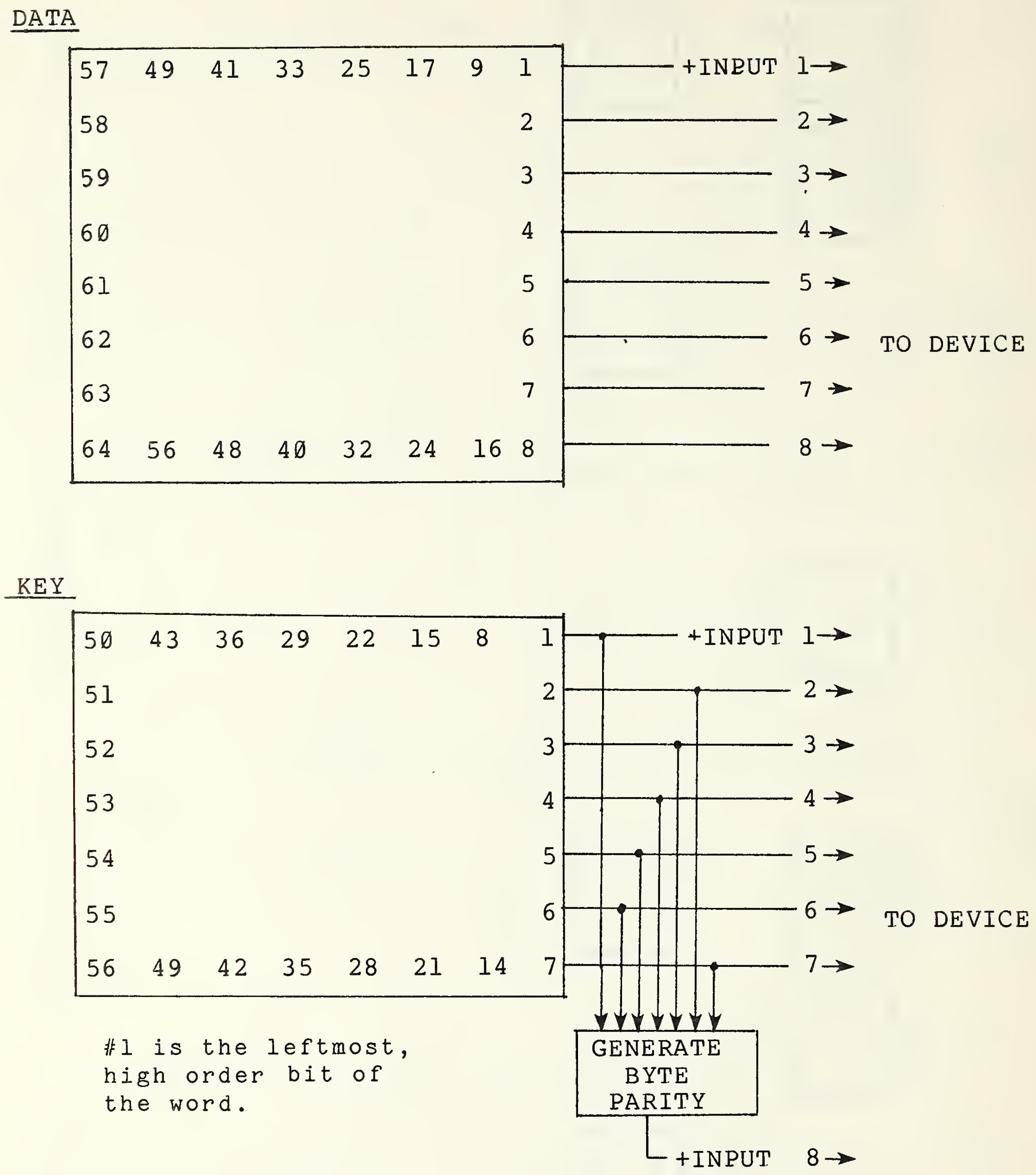
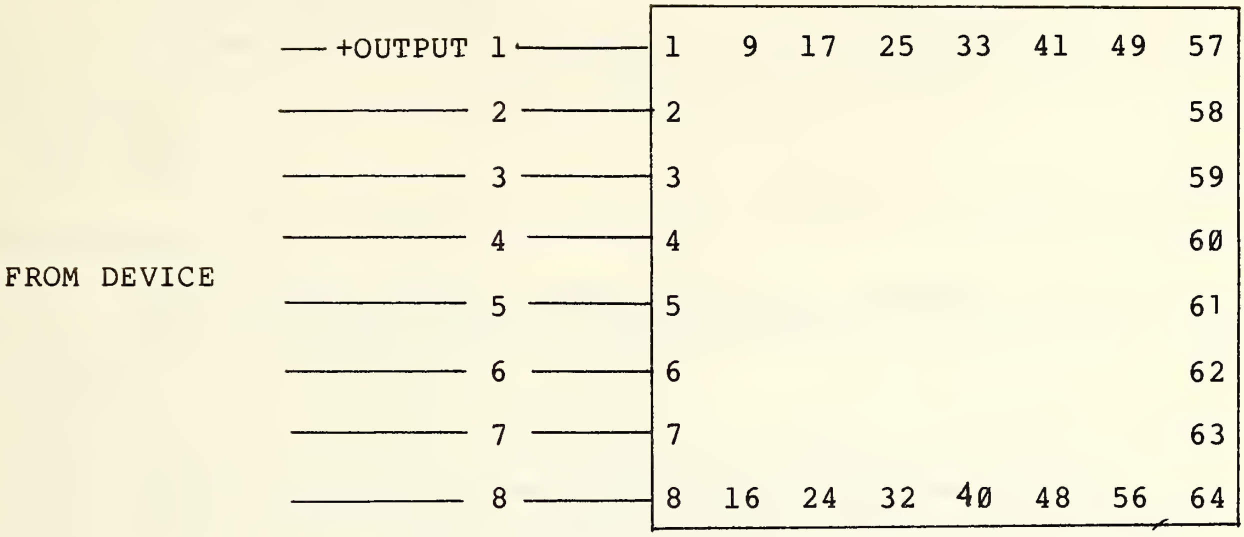


Figure C2 . The logic diagram for the NBS data encryption testbed interface.



#1 is the leftmost, high order bit of the word.

Figure C3 . Input data and input key byte numbering for the NBS data encryption standard testbed interface.



#1 is the leftmost,high order bit of the 64-bit data block.

Fiqure C4 . Output data byte numbering for the NBS data encryption testbed interface.

REFERENCES

1. Meyer, C., Enciphering Data for Secure Transmission, Computer Design,(April, 1974)129-34.

2. Meyer, C. and W. Tuchman, Pseudo-random Codes Can Be Cracked, Elect. Design,vol. 23(1972)74-6.

3. Data Encryption Standard, FIPS PUB 46, Jan. 15, 1977.

4. Grossman, E. and B. Tuckerman, Analysis of a Feistel-like Cipher Weakened by Having No Rotating Key, IBM Rpt c6375, 1977.

5. Gait, J., A New Non-Linear Pseudo-random Number Generator, IEEE Transactions on Software Engineering, Sept.,1977.

6. Bright, H. and R. Ennison; Cryptography Using Modular Software Elements, National Computer Conf.,1976,113-23.

7. Calibration and Test Services of NBS,Spec.Pub. 25Ø,197Ø.

8. DES Guidelines,NBS Special Publication 5ØØ-xx (In preparation).

U.S. DEPT. OF COMM. BIBLIOGRAPHIC DATA SHEET	1. PUBLICATION OR REPORT NO. NBS SP 500-20	2. Gov't Accession No.	3. Recipient's Accession No.

4. TITLE AND SUBTITLE

COMPUTER SCIENCE & TECHNOLOGY:

Validating the Correctness of Hardware Implementations of the NBS Data Encryption Standard

5. Publication Date

November 1977

6. Performing Organization Code

7. AUTHOR(S)

Jason Gait

8. Performing Organ. Report No.

9. PERFORMING ORGANIZATION NAME AND ADDRESS

NATIONAL BUREAU OF STANDARDS
DEPARTMENT OF COMMERCE
WASHINGTON, D.C. 20234

10. Project/Task/Work Unit No.

11. Contract/Grant No.

12. Sponsoring Organization Name and Complete Address *(Street, City, State, ZIP)*

Same as Number 9.

13. Type of Report & Period Covered

14. Sponsoring Agency Code

15. SUPPLEMENTARY NOTES

Library of Congress Catalog Card Number: 77-16067

16. ABSTRACT *(A 200-word or less factual summary of most significant information. If document includes a significant bibliography or literature survey, mention it here.)*

This publication describes the design and operation of the NBS testbed that is used for the validation of hardware implementations of the Federal Information Processing Data Encryption Standard (DES). A particular implementation is verified if it correctly performs a set of 291 test cases that have been defined to exercise every basic element of the algorithm. As a further check on the correctness of the implementation an extensive Monte-Carlo test is performed. This publication includes the full specification of the DES algorithm, a complete listing of the DES test set and a detailed description of the interface to the testbed.

17. KEY WORDS *(six to twelve entries; alphabetical order; capitalize only the first letter of the first key word unless a proper name; separated by semicolons)*

Communications security; computer security; cryptography; encryption standard; interface requirements; Monte-Carlo testing; testbed; test cases; validating correctness.

18. AVAILABILITY ☒ Unlimited

□ For Official Distribution. Do Not Release to NTIS

☒ Order From Sup. of Doc., U.S. Government Printing Office
Washington, D.C. 20402, SD Cat. No. C13.10:500-20

□ Order From National Technical Information Service (NTIS)
Springfield, Virginia 22151

19. SECURITY CLASS (THIS REPORT)

UNCLASSIFIED

20. SECURITY CLASS (THIS PAGE)

UNCLASSIFIED

21. NO. OF PAGES

46

22. Price

$1.60

☆U.S. GOVERNMENT PRINTING OFFICE: 1977-261-238/379

ANNOUNCEMENT OF NEW PUBLICATIONS ON COMPUTER SCIENCE & TECHNOLOGY

Superintendent of Documents,
Government Printing Office,
Washington, D. C. 20402

Dear Sir:

Please add my name to the announcement list of new publications to be issued in the series: National Bureau of Standards Special Publication 500-.

Name ____

Company ____

Address ____

City ____________________ State ______________ Zip Code __________

(Notification key N-503)

NBS TECHNICAL PUBLICATIONS

PERIODICALS

JOURNAL OF RESEARCH—The Journal of Research of the National Bureau of Standards reports NBS research and development in those disciplines of the physical and engineering sciences in which the Bureau is active. These include physics, chemistry, engineering, mathematics, and computer sciences. Papers cover a broad range of subjects, with major emphasis on measurement methodology, and the basic technology underlying standardization. Also included from time to time are survey articles on topics closely related to the Bureau's technical and scientific programs. As a special service to subscribers each issue contains complete citations to all recent NBS publications in NBS and non-NBS media. Issued six times a year. Annual subscription: domestic $17.00; foreign $21.25. Single copy, $3.00 domestic; $3.75 foreign.

Note: The Journal was formerly published in two sections: Section A "Physics and Chemistry" and Section B "Mathematical Sciences."

DIMENSIONS/NBS (formerly Technical News Bulletin)—This monthly magazine is published to inform scientists, engineers, businessmen, industry, teachers, students, and consumers of the latest advances in science and technology, with primary emphasis on the work at NBS. The magazine highlights and reviews such issues as energy research, fire protection, building technology, metric conversion, pollution abatement, health and safety, and consumer product performance. In addition, it reports the results of Bureau programs in measurement standards and techniques, properties of matter and materials, engineering standards and services, instrumentation, and automatic data processing.

Annual subscription: Domestic, $12.50; Foreign $15.65.

NONPERIODICALS

Monographs—Major contributions to the technical literature on various subjects related to the Bureau's scientific and technical activities.

Handbooks—Recommended codes of engineering and industrial practice (including safety codes) developed in cooperation with interested industries, professional organizations, and regulatory bodies.

Special Publications—Include proceedings of conferences sponsored by NBS, NBS annual reports, and other special publications appropriate to this grouping such as wall charts, pocket cards, and bibliographies.

Applied Mathematics Series—Mathematical tables, manuals, and studies of special interest to physicists, engineers, chemists, biologists, mathematicians, computer programmers, and others engaged in scientific and technical work.

National Standard Reference Data Series—Provides quantitative data on the physical and chemical properties of materials, compiled from the world's literature and critically evaluated. Developed under a world-wide program coordinated by NBS. Program under authority of National Standard Data Act (Public Law 90-396).

NOTE: At present the principal publication outlet for these data is the Journal of Physical and Chemical Reference Data (JPCRD) published quarterly for NBS by the American Chemical Society (ACS) and the American Institute of Physics (AIP). Subscriptions, reprints, and supplements available from ACS, 1155 Sixteenth St. N.W., Wash., D.C. 20056.

Building Science Series—Disseminates technical information developed at the Bureau on building materials, components, systems, and whole structures. The series presents research results, test methods, and performance criteria related to the structural and environmental functions and the durability and safety characteristics of building elements and systems.

Technical Notes—Studies or reports which are complete in themselves but restrictive in their treatment of a subject. Analogous to monographs but not so comprehensive in scope or definitive in treatment of the subject area. Often serve as a vehicle for final reports of work performed at NBS under the sponsorship of other government agencies.

Voluntary Product Standards—Developed under procedures published by the Department of Commerce in Part 10, Title 15, of the Code of Federal Regulations. The purpose of the standards is to establish nationally recognized requirements for products, and to provide all concerned interests with a basis for common understanding of the characteristics of the products. NBS administers this program as a supplement to the activities of the private sector standardizing organizations.

Consumer Information Series—Practical information, based on NBS research and experience, covering areas of interest to the consumer. Easily understandable language and illustrations provide useful background knowledge for shopping in today's technological marketplace.

Order **above** *NBS publications from: Superintendent of Documents, Government Printing Office, Washington, D.C. 20402.*

Order **following** *NBS publications—NBSIR's and FIPS from the National Technical Information Services, Springfield, Va. 22161.*

Federal Information Processing Standards Publications (FIPS PUB)—Publications in this series collectively constitute the Federal Information Processing Standards Register. Register serves as the official source of information in the Federal Government regarding standards issued by NBS pursuant to the Federal Property and Administrative Services Act of 1949 as amended, Public Law 89-306 (79 Stat. 1127), and as implemented by Executive Order 11717 (38 FR 12315, dated May 11, 1973) and Part 6 of Title 15 CFR (Code of Federal Regulations).

NBS Interagency Reports (NBSIR)—A special series of interim or final reports on work performed by NBS for outside sponsors (both government and non-government). In general, initial distribution is handled by the sponsor; public distribution is by the National Technical Information Services (Springfield, Va. 22161) in paper copy or microfiche form.

BIBLIOGRAPHIC SUBSCRIPTION SERVICES

The following current-awareness and literature-survey bibliographies are issued periodically by the Bureau:

Cryogenic Data Center Current Awareness Service. A literature survey issued biweekly. Annual subscription: Domestic, $25.00; Foreign, $30.00.

Liquified Natural Gas. A literature survey issued quarterly. Annual subscription: $20.00.

Superconducting Devices and Materials. A literature survey issued quarterly. Annual subscription: $30.00. Send subscription orders and remittances for the preceding bibliographic services to National Bureau of Standards, Cryogenic Data Center (275.02) Boulder, Colorado 80302.

U.S. DEPARTMENT OF COMMERCE
National Bureau of Standards
Washington, D.C. 20234